

United States District Court
Northern District of California

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MICHAEL KATZ-LACABE, et al.,
Plaintiffs,
v.
ORACLE AMERICA, INC.,
Defendant.

Case No. [22-cv-04792-RS](#)

**ORDER GRANTING IN PART AND
DENYING IN PART MOTION TO
DISMISS AND GRANTING IN PART
AND DENYING IN PART MOTION TO
FILE UNDER SEAL**

I. INTRODUCTION

On April 6, 2023, Defendant Oracle America, Inc.’s (“Oracle”) motion to dismiss Plaintiffs’ initial complaint was granted in part and denied in part. *See* Order Granting in Part and Denying in Part Defendant’s Motion to Dismiss (“4/6 Order”). Now, in their First Amended Class Action Complaint (“FAC”), two individual Plaintiffs bring this putative class action against Oracle, alleging the company violates internet users’ right to privacy as that right is enshrined under the California Constitution and various state and federal privacy statutes. Defendant moves to dismiss many of Plaintiffs’ claims under Federal Rules of Civil Procedure 12(b)(6) for failure to state a claim or to comply with Federal Rule of Civil Procedure 8. Plaintiffs also filed a motion to seal portions of the Offline Access Request Response Reports (OARRRs). For the reasons that follow, both the motion to dismiss and motion to seal are granted in part and denied in part. These motions are suitable for disposition without oral argument, and the motion hearing set for October 5, 2023, is vacated. *See* Civ. L.R. 7-1(b).

II. BACKGROUND¹

Plaintiffs in this case are two named individuals—Michael Katz-Lacabe, a resident of San Leandro, California, and Dr. Jennifer Golbeck, a resident of Sugarloaf Key, Florida—who purport to represent six separate classes of individuals in a suit against Oracle. Despite taking precautions to maintain privacy and prevent third-party collection of their data, Plaintiffs each received a document from Oracle (an OARRR) indicating that Oracle had tracked, compiled, and analyzed their web browsing and other activity, thereby creating an “electronic profile” of them. *See* Dkt. 54 at 2, 6. Further, Plaintiffs aver Oracle tracks their internet activity across numerous websites with various technological tools, their location through partnership with the company PlaceIQ, and their financial data, and then makes that information available to third parties without Plaintiffs’ consent.

Plaintiffs explain that Oracle collects data using a number of tools, including: (1) cookies (pieces of software code stored on web browsers that collect users’ data, like IP addresses); (2) the javascript code “bk-coretag.js” (proprietary code which copies and sends to Oracle what information users are requesting from a website server, such as a URL, date and time of visit, and webpage keywords); (3) tracking pixels (code embedded into webpages that track information whenever the webpage is opened); (4) device identification; (5) cross-device tracking; (6) AddThis widgets; and (7) Datalogix (an information broker specializing in profiles built from brick and mortar purchases). As in their initial complaint, Plaintiffs take issue with Oracle’s extensive data brokering business. In so doing, Plaintiffs focus on two key features of Defendant’s data management platform (BlueKai Data Management Platform): (1) the Oracle Data Marketplace, allegedly one of the world’s largest commercial data exchanges; and (2) the Oracle ID Graph. Plaintiffs aver Defendant’s business model proceeds as follows: first, Oracle collects as many

¹ The factual background of this case is based on the well-pled allegations in the First Amended Class Action Complaint (“FAC”), which are taken as true for the purposes of this motion. This background is presented in greater detail in the 4/6 Order given the substantial factual overlap between the original complaint and the FAC.

types of personal information from internet users as possible. Then, Oracle synchronizes that data to create individual profiles, analyzes the data, and monetizes the data by selling it on its Data Marketplace. Plaintiffs argue that neither Oracle’s privacy policies, nor the privacy policies of third-party publishers, provide a basis to conclude that Plaintiffs consented to this data collection, curation, and monetization.

In the 4/6 Order, Plaintiffs’ Unfair Competition Law (UCL), Federal Wiretap Act, unjust enrichment, and intrusion upon seclusion (on behalf of national and international sub-classes) claims were dismissed, while Plaintiffs’ invasion of privacy, intrusion upon seclusion (for the California sub-class), California Invasion of Privacy Act (CIPA), and declaratory judgment and equitable relief claims survived. Plaintiffs filed their FAC on May 22, 2023, bringing some new claims, dropping their UCL claim, and adding factual averments in support of other claims. Oracle moved to dismiss most, but not all, of Plaintiffs’ claims. Additionally, Plaintiffs filed a motion to seal portions of the OARRRs on September 19, 2023, which Defendant opposes.

III. MOTION TO DISMISS

A. Legal Standard

A complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). While “detailed factual allegations” are not required, a complaint must have sufficient factual allegations to state a claim that is “plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 570 (2007)). A claim is facially plausible “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* (citing *Twombly*, 550 U.S. at 556). This standard asks for “more than a sheer possibility that a defendant has acted unlawfully.” *Id.* The determination is a context-specific task requiring the court “to draw on its judicial experience and common sense.” *Id.* at 679.

A Rule 12(b)(6) motion to dismiss tests the sufficiency of the claims alleged in the complaint. Dismissal under Rule 12(b)(6) may be based on either the “lack of a cognizable legal theory” or on “the absence of sufficient facts alleged under a cognizable legal theory.” *See*

Conservation Force v. Salazar, 646 F.3d 1240, 1242 (9th Cir. 2011) (internal quotation marks and citation omitted). When evaluating such a motion, the court must accept all material allegations in the complaint as true and construe them in the light most favorable to the non-moving party. *In re Quality Sys., Inc. Sec. Litig.*, 865 F.3d 1130, 1140 (9th Cir. 2017). It must also “draw all reasonable inferences in favor of the nonmoving party.” *Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987).

B. Discussion

Plaintiffs claim to represent six different potential classes of plaintiffs: the United States Class,² the California Sub-Class,³ the California Invasion of Privacy Act (CIPA) Sub-Class,⁴ the Florida Sub-Class,⁵ the Florida Security of Communications Act (FSCA) Sub-Class,⁶ and the Electronic Communications Privacy Act (ECPA) Sub-Class.⁷

On behalf of these classes, the FAC alleges nine causes of action: (1) Invasion of Privacy under the California Constitution (for the California Sub-Class); (2) Intrusion Upon Seclusion under California Common Law (on behalf of the United States Class, or in the alternative, the California Sub-Class); (3) Intrusion Upon Seclusion under Florida Common Law (in the

² “All natural persons located in the United States whose personal information, or data derived from their personal information, was used to create a profile and made available for sale or use through Oracle’s ID Graph or Data Marketplace.”

³ “All natural persons located in California whose personal information, or data derived from their personal information, was used to create a profile and made available for sale or use through Oracle’s ID Graph or Data Marketplace.”

⁴ “All members of the California Sub-Class whose contents of their electronic communications were intercepted by the use of Oracle’s bk-coretag.js functionality.”

⁵ “All natural persons located in Florida whose personal information, or data derived from their personal information, was used to create a profile and made available for sale or use through Oracle’s ID Graph or Data Marketplace.”

⁶ “All members of the Florida Sub-Class whose contents of their electronic communications were intercepted by the use of Oracle’s bk-coretag.js functionality.”

⁷ “All members of the United States Sub-Class whose contents of their electronic communications were intercepted by the use of Oracle’s bk-coretag.js functionality.”

alternative, for the Florida Sub-Class); (4) Violation of the California Invasion of Privacy Act (on behalf of the CIPA Sub-Class); (5) Violation of the FSCA, under Fla. Stat. § 934.03 (for the FSCA Sub-Class); (6) Violation of the Federal Wiretap Act, under 18 U.S.C. § 2510 (for the ECPA Sub-Class); (7) Unjust Enrichment, under California Common Law (on behalf of the United States Class, or in the alternative, the California Sub-Class); (8) Unjust Enrichment, under Florida Common Law (in the alternative, for the Florida Sub-Class); and (9) Declaratory Judgment and Injunctive Relief (on behalf of all classes).

Defendant moves to dismiss all claims—with the exception of Plaintiffs’ first and second claims, to the extent the second claim is brought against the California Sub-Class—under Rule 12(b)(6).

1. Second Cause of Action: Intrusion Upon Seclusion

First, Oracle moves to dismiss Plaintiffs’ second cause of action to the extent Plaintiffs attempt to assert a California state claim on behalf of a non-California resident (Golbeck) and a class inclusive of non-California residents (the United States Class). The prior order found that Plaintiffs failed to show why California law should be applied nationwide for its intrusion upon seclusion claim. *See* 4/6 Order. Plaintiffs contend they have augmented that claim with averments which justify applying California law to the nationwide class and that, to the extent Oracle disputes those allegations, Oracle merely raises a factual dispute inappropriate for resolution at the motion to dismiss stage.

Plaintiffs argue the “last acts” necessary to make Oracle liable on an intrusion upon seclusion claim occurred in California because it was in California that Oracle compiled, analyzed, and sold their data. Dkt. 67, at 19–20. Defendant persuasively points out, however, that Plaintiffs’ own allegations identify the last act necessary for liability to attach to be Oracle’s interception of Plaintiffs’ data. *See* Dkt. 70, at 2; FAC ¶ 145. Plaintiffs’ theory of liability for intrusion upon seclusion would make Oracle liable when it intercepted Plaintiffs’ data, and Plaintiffs do not offer any reason to doubt that this interception of data, for non-California residents, occurs in those residents’ home States. *See Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 593 (9th Cir. 2012)

(“California considers the ‘place of the wrong’ to be the state where the last event necessary to make the actor liable occurred.”), *overruled on other grounds by Olean Wholesale Grocery Coop. v. Bumble Bee Foods LLC*, 31 F.4th 651 (9th Cir. 2022). Since the last act at which liability attaches—here, interception of Plaintiff Golbeck’s data—occurred in Florida, this factor weighs against applying California law nationwide. *See, e.g., Hayden v. Retail Equation, Inc.*, No. 20-cv-1203, 2022 WL 18397355, at *5 (C.D. Cal. Nov. 28, 2022) (finding California law inapplicable to privacy claims where “collection and transmission” of data occurred outside California).

Plaintiffs’ amended averments in their FAC do not warrant a different conclusion than the one reached in this Court’s 4/6 Order: namely, that California law does not apply nationwide for Plaintiffs’ intrusion upon seclusion claim. Therefore, Plaintiffs’ intrusion upon seclusion claim—to the extent it is brought on behalf of the United States Class under California law, as opposed to solely on behalf of the California Sub-Class—is dismissed without leave to amend.

2. Third Cause of Action: Intrusion Upon Seclusion (Florida Common Law)

Plaintiffs, in the alternative, bring a claim for intrusion upon seclusion under Florida law on behalf of the Florida-Class. To state a claim for intrusion upon seclusion under Florida law, a plaintiff must show an intrusion onto a private place that would be highly offensive to a reasonable person. *Hammer v. Sorensen*, 824 F. App’x 689, 695 (11th Cir. 2020). Intrusions can be either physical or electronic. *See Spilfogel v. Fox Broadcasting Co.*, 724, 726 (11th Cir. 2011). The requirement in Florida that a plaintiff must “show an intrusion into a private place and not merely a private activity” goes beyond the Restatement (Second) of Torts, which has no such “private place” requirement. *Id.* (citing *Allstate Ins. Co. v. Ginsberg*, 863 So. 2d 156, 161 n.3, 162 (Fla. 2003)).

As a general matter, courts have declined to extend Florida’s protections against the invasion of privacy tort (of which intrusion upon seclusion is a subtype) to instances in which a party accesses digital files. *See Celestine v. Capital One*, No. 17-cv-20237, 2017 WL 2838185, at *3 (S.D. Fla. June 30, 2017) (accessing a credit report does not constitute intrusion into a “place”); *Bradley v. City of St. Cloud*, No. 12-cv-1348, 2013 WL 3270403, at *5 (M.D. Fla. June 26, 2013)

(similar, for medical records). In the FAC, Plaintiff Golbeck avers Oracle’s data collection constitutes an intrusion into her home and her computer. FAC ¶ 163. Additionally, Plaintiffs cite *Hammer* for the proposition that “private quarters” can include “electronic space.” Dkt. 67, at 22. Defendant responds that *Hammer*’s reference to a potentially private email address is not analogous to “open conduct on the web.” Dkt. 70, at 5 n.11. Defendant argues non-private internet activity does not occur in a “private place,” *id.*, and Plaintiff Golbeck seems to acknowledge the lack of cases finding collection of browsing data constitutes an intrusion into a private quarter, Dkt. 67, at 23 (“No Florida case addresses any fact pattern that comes close to resembling the one at bar.”). *See, e.g., Rebalko v. City of Coral Springs*, 552 F. Supp. 3d 1285, 1333 (S.D. Fla. 2020) (noting Florida courts have said “precious little” about what places, beyond a home, constitute a private quarter).

Oracle has the better of this dispute. Accepting that an electronic space may constitute a “private quarter,” *see Spilfogel v. Fox Broadcasting Co.*, No. 9-cv-80813, 2010 WL 11504189, at *5 (S.D. Fla. May 4, 2010), Plaintiffs do not plausibly point to any particular “electronic space” where Plaintiff Golbeck had a reasonable expectation of privacy into which Oracle intruded. Nor do Plaintiffs plausibly aver Oracle intruded into Plaintiff Golbeck’s home. Thus, Plaintiffs have not alleged sufficient facts to state a claim for intrusion upon seclusion under Florida law because they have not alleged an intrusion into a “private place” or “private quarter.” For this reason, Plaintiffs’ intrusion upon seclusion claim brought under Florida law must be dismissed with leave to amend.

3. Fourth, Fifth, and Sixth Causes of Action: CIPA (California), FSCA (Florida), and ECPA (Federal Wiretap Act)

i. CIPA

Defendant argues Plaintiffs’ CIPA claim should be dismissed (1) because Plaintiffs do not sufficiently allege Defendant had the requisite intent to violate CIPA or, in the alternative, (2) to the extent the claim is premised on collection of the seven types of information this Court

previously determined do not qualify as “contents.”⁸

First, Oracle points to California Penal Code § 631(a)’s requirement that contents subject to CIPA be read (or attempted to be read) “willfully and without the consent of all parties to the communication” and argues Plaintiffs have not pled sufficient facts Oracle had the requisite intent here. Dkt. 63, at 16. Recording a confidential communication is intentional where the recording entity has the “purpose or desire” of recording the communication or the “knowledge to a substantial certainty” the communication will be recorded. *People v. Sup. Ct. (Smith)*, 449 P.2d 230, 238 (Cal. 1969). Defendant cites *Lozano v. City of Los Angeles*, 73 Cal. App. 5th 711, 727–28 (Cal. Ct. App. 2022), as support for its position that the recording tool at issue here (the bk-coretag.js) would not necessarily record the content of communications as opposed to record information. Dkt. 63, at 17. Oracle further contends the causal chain of intention is broken by the fact that its customers “choose what portion of the collected data they wish to share with Oracle” and to obtain consent to collect the information from users. *See id.* at 17–18.⁹

Plaintiffs, however, have sufficiently alleged Oracle had “knowledge to a substantial certainty” that deployment of the bk-coretag.js would record confidential communications. *See, e.g., Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 690 (N.D. Cal. 2021) (finding intent requirement satisfied given Apple’s knowledge “accidental Siri triggers” would, with substantial certainty, “occur in confidential contexts”). Plaintiffs aver Oracle’s products—such as the bk-coretag.js—are implemented by websites and collect vast quantities of personal information that eventually makes its way back to Oracle. *See, e.g., FAC* ¶¶ 44–46. Plaintiffs further claim this data collection occurs despite Oracle’s knowledge that many users do not consent to it. *See, e.g., id.* ¶¶ 59, 107–108. Such averments, like those in *Lopez*, are sufficient at this stage to satisfy the intent requirement.

⁸ Those categories are webpage titles, webpage keywords, the date and times of website visits, IP addresses, page visits, purchase intent signals, and add-to-cart actions. These categories of data are not “content” regardless of whether Plaintiffs actually conceded the issue. *See, e.g., Dkt. 67*, at 5.

⁹ This “chain of causation” argument echoes the Article III standing arguments Oracle made in its previous motion to dismiss.

Second, solely to the extent Plaintiffs' CIPA claim avers referrer URLs and data entered into forms are "content," Plaintiffs have met their burden (as they did on Defendant's first motion to dismiss) to plead sufficient facts to withstand dismissal. Therefore, Plaintiffs' CIPA claim survives.

ii. FSCA

Oracle moves to dismiss Plaintiffs' FSCA claim for failure to state a claim on two primary grounds: (1) information obtained by the bk-coretag.js is not "electronic communication" as defined by the statute and (2) Plaintiffs lack a reasonable expectation of privacy in the information. Dkt. 63, at 18–21. Neither argument persuades.

The histories of the FSCA and the Federal Wiretap Act are instructive regarding what constitutes electronic communication. As Oracle acknowledges, the Florida Legislature amended the FSCA (extending the statute to cover "electronic communication") in tandem with Congress's similar modification of the Federal Wiretap Act. *See* Dkt. 63, at 20; *see also State v. Jackson*, 650 So.2d 24, 27 (Fla. 1995) (similar). The Federal Wiretap Act and FSCA appear to define "electronic communication" identically. *Compare* 18 U.S.C. § 2510(12) *with* Fla. Stat. § 934.02(12). While Defendant is correct that both statutes exclude any device which "permits the tracking of the movement of a person or an object," *see, e.g.,* Fla. Stat. § 934.02(12)(c), the cases Defendant cites relate primarily to the use of session replay software. *See, e.g., Jacome v. Spirit Airlines Inc.*, No. 2021-947, 2021 WL 3087860, at *3 (Fla. Cir. Ct. June 17, 2021). Plaintiffs respond that the bk-coretag.js is script not analogous to such software, *see* Dkt. 67, at 21, a contention Oracle disputes on the grounds the two tools capture the same types of information, *see* Dkt. 70, at 10.

Plaintiffs have the better of this disagreement. Fla. Stat. § 934.02(12)(c) specifically excludes from its definition of electronic communications any communications from a "device which permits the tracking of *the movement of a person or an object*" (emphasis added). Oracle does not claim the bk-coretag.js literally tracks "movement" within the meaning of the statute. Second, Oracle's argument that what matters is whether the bk-coretag.js captures the "same

information” as session replay software goes too far. The First Circuit, for instance, has already interpreted the Federal Wiretap Act’s definition of electronic communication to include “[t]ransmissions of completed online forms.” *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003). In so doing, it noted the Act “adopts a ‘broad, functional’ definition of an electronic communication.” *Id.* (quoting *Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995)). This definition of “electronic communication” is sufficiently broad to encompassreferrer URLs. Therefore, to the extent the FSCA tracks the Federal Wiretap Act, at least some of the transmissions the bk-coretag.js allegedly captured—transmissions containing “data entered by the user into forms” on various websites, FAC ¶¶ 183, and referrer URLs—constitute electronic communications under the FSCA.

Second, assuming (without deciding) Defendant is correct Plaintiffs must have a reasonable expectation of privacy in electronic communications under the FSCA,¹⁰ Plaintiffs have met this burden. One of Plaintiffs’ central contentions is that users do not actually consent to either Defendant’s or third-party websites’ collection of information about their internet browsing and that they had a corresponding privacy interest in that information. Plaintiffs have sufficiently pled a reasonable expectation of privacy in at least some of the information they aver Defendant compiled through an extensive data collection and profiling scheme. Thus, Plaintiffs’ FSCA claim survives.

iii. ECPA

Plaintiffs add averments to their FAC, *see* FAC ¶¶ 226–230, in a renewed attempt to

¹⁰ Plaintiffs persuasively argue the FSCA does not require a reasonable expectation of privacy in electronic communications. In *Brevard Extraditions, Inc. v. Fleetmatics, USA, LLC*, the court noted the different definitions of “wire communication” and “oral communication” in the FSCA, the explicit reference to privacy expectations in the statute’s definition of the latter, *see* Fla. Stat. § 934.02(2), and the fact that wire communications are “generally protected regardless of whether the person making or receiving the communication has an expectation of privacy.” No. 12-cv-2079, 2013 WL 5437117, at *4 (M.D. Fla. Sept. 27, 2013) (citing *PBA Local No. 38 v. Woodbridge Police Dep’t*, 832 F. Supp. 808 (D.N.J. 1993)). Section 934.02(12) of the FSCA, which defines “electronic communication”—like the definition of “wire communication” and unlike the definition of “oral communication”—contains no reference to expectations of privacy.

demonstrate “the primary motivation or a determining factor in [Oracle’s] actions” in the context of intercepting communications “has been to injure plaintiffs tortiously.” *See Rodriguez v. Google LLC*, No. 20-cv-04688-RS, 2021 WL 2026726, at *6 n.8 (N.D. Cal. May 21, 2021) (declining to apply crime-fraud exception where company did not intend to injure plaintiffs tortiously) (citing *In re Google Inc. Gmail Litig.*, No. 13-md-02430, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014)). As support for their claim, Plaintiffs (1) cite Oracle CEO Larry Ellison’s comments about how the company’s data-collection abilities were “scaring the lawyers” and (2) argue the goal of “making money” cannot sanitize tortious conduct. FAC ¶¶ 227-28. Without more, Plaintiffs have not alleged sufficient facts that Oracle intercepted data with the primary motivation or purpose of committing torts on internet users.¹¹

Plaintiffs cite *Brown v. Google, LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021)—a case where the crime-fraud exception was found to apply—and argue this case is analogous. Defendant effectively distinguishes this case and *Brown*; for instance, Defendant points out how the plaintiffs in *Brown* had identified internal Google communications referring to the company’s privacy practices as problematic. Dkt. 70, at 11; *Brown*, 525 F. Supp. 3d at 1079; *see also In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (finding failure to show necessary wrongful intent). Plaintiffs have not pled sufficient facts here to show Oracle had tortious motivation. Thus, for the reasons discussed in this Court’s prior order dismissing Plaintiffs’ ECPA claim in light of Defendant’s consent defense, Plaintiffs’ ECPA claim must be dismissed. *See* 4/6 Order, at 16.

4. Seventh & Eighth Causes of Action: Unjust Enrichment

i. Unjust enrichment under California law

Plaintiffs’ FAC successfully pleads an unjust enrichment cause of action under California

¹¹ The mere possibility Oracle’s data collection activities could at some future date be deemed tortious does not justify application of the crime-fraud exception in these circumstances. *See, e.g., In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 518–19 (S.D.N.Y. 2001) (noting “a culpable mind does not accompany every tortious act”).

law. In order “[t]o allege unjust enrichment as an independent cause of action, a plaintiff must show that the defendant received and unjustly retained a benefit at the plaintiff’s expense.” *ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016). The benefit Plaintiffs claim Oracle received and retained here is information—both from third-party websites and independently collected—about Plaintiffs’ online and real-world lives.

Plaintiffs now aver they “were not aware of Oracle’s conduct while browsing websites” (ostensibly websites incorporating the `bk-coretag.js` or other Oracle technology), and “would not have visited those websites” or, in the alternative, would have taken steps while visiting the websites “to avoid being tracked and profiled by Oracle.”¹² FAC ¶ 249(a). Oracle’s collection of data from third-party websites, Plaintiffs argue, conferred a benefit upon Oracle at the expense of the privacy of their data. *Id.* ¶ 248–249. Plaintiffs also allege Defendant has collected their real-world location information, and then compiled and sold that information, without their consent. *Id.* ¶ 249(b)–(c). With their added averments, Plaintiffs have done just enough for their unjust enrichment cause of action under California law to survive.

ii. Choice of law

Defendant argues Plaintiffs cannot assert an unjust enrichment claim under California state law on behalf of non-California residents—on behalf of either a named plaintiff, Golbeck (a Florida resident), or classes inclusive of non-residents, such as the United States class—and seeks dismissal of Plaintiffs’ claims to that extent.

As before, both parties agree “[a] federal court sitting in diversity must look to the forum state’s choice of law rules,” thus requiring the court to apply California’s “governmental interest approach” to determine questions of choice of law. *Zinser v. Accufix Resch. Inst., Inc.*, 253 F.3d 1180, 1187 (9th Cir. 2001). This is a three-step process. The first task is to determine whether the

¹² Plaintiffs also cite *Brooks v. Thomson Reuters Corp.* as persuasive authority for allowing an unjust enrichment claim to proceed in the context of a data broker’s alleged violation of privacy rights. No. 21-cv-1418, 2021 WL 3621837, at *11–12 (N.D. Cal. Aug. 16, 2021). There, however, the court merely rejected defendant’s argument regarding whether unjust enrichment can be asserted as a standalone cause of action. *Id.* at *11.

laws of the affected jurisdictions are “the same or different.” *Mazza*, 666 F.3d at 590 (quoting *McCann v. Foster Wheeler LLC*, 48 Cal. 4th 68, 81-82 (2010)). If the laws are different, the second step requires an examination of “each jurisdiction’s interest in the application of its own law” to determine whether a true conflict exists. *Id.* If it does, then the final step involves analyzing “which state’s interest would be more impaired if its policy were subordinated to the policy of the other state.” *Id.*

First, Oracle persuasively contends California and Florida have significantly different standards for unjust enrichment claims on the grounds that Florida—but not California—requires (1) the recipient of a benefit to have “knowledge” of and to “accept” the benefit and (2) that the benefit be *directly* conferred on the defendant. *See* Dkt. 63, at 7; *see also Kopel v. Kopel*, 229 So.3d 812, 818 (Fla. 2017) (“the plaintiff must directly confer a benefit to the defendant”). It is possible an unjust enrichment claim could succeed in California but fail in Florida on the grounds the conferred benefit was insufficiently direct. *See Gustafson v. BAC Home Loans Servicing, LP*, 294 F.R.D. 529, 548 (C.D. Cal. 2013); *see also Virgilio v. Ryland Group, Inc.*, 680 F.3d 1329, 1337 (11th Cir. 2012) (finding third party, and not the plaintiffs, conferred the relevant benefit where third party “bargained away” its rights to the benefit). As Oracle notes, the Ninth Circuit has held the “elements necessary to establish a claim for unjust enrichment also vary materially from state to state.” *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 591 (9th Cir. 2012). Though Plaintiffs represent they will offer the same proof under either California’s or Florida’s test, this does not alter the fact that the two States have materially different standards.

Next, a true conflict exists. Florida has a strong interest in determining how to balance protecting consumers and attracting business. *See, e.g., Mazza*, 66 F.3d at 591–93. Florida indisputably has an interest in applying its own consumer protection laws to its own residents. Third, California’s interest in applying its unjust enrichment law to non-California residents is attenuated. *See In re Toyota RAV4 Hybrid Fuel Tank Litig.*, 534 F. Supp. 3d 1067, 1122 (N.D. Cal. 2021) (applying *Mazza*). As in *Mazza* and *In re Toyota*, the States in which relevant transactions occur have the stronger interest in policing those transactions. For these reasons,

1 Plaintiffs’ unjust enrichment claim under California law on behalf of the United States Class
 2 cannot stand. Plaintiffs’ unjust enrichment claim under California law on behalf of the United
 3 States Class is dismissed with leave to amend.

4 **iii. Florida law (*eighth cause of action*)**

5 Given the survival of Plaintiffs’ unjust enrichment claim under California law and the fact
 6 California law cannot be applied to the United States Class, it is necessary to assess Plaintiffs’
 7 unjust enrichment cause of action pled, in the alternative, under Florida law. Plaintiffs bring this
 8 cause of action on behalf of the Florida Sub-Class. To state a claim for unjust enrichment in
 9 Florida, a plaintiff must show the plaintiff directly conferred a benefit on the defendant. *Kopel*,
 10 229 So.3d at 818. Further, the plaintiff must show the defendant voluntarily accepted and retained
 11 the benefit and that it would be inequitable for the defendant to retain the benefit without
 12 compensating the plaintiff. *Peoples Nat. Bank of Commerce v. First Union Nat. Bank of Fla.*, 667
 13 So.2d 876, 879 (Fla. Dist. Ct. App. 1996).

14 Oracle first contends Plaintiffs received the benefit of their bargain because they were able
 15 to access third-party websites despite the collection of their data. Plaintiffs, as they did for their
 16 unjust enrichment claim under California law, have added sufficient averments to the FAC to
 17 explain why the access they gained to third-party websites does not defeat their claim. Oracle also
 18 posits that Plaintiffs have failed to show any direct conferral of a benefit because Oracle’s
 19 customers are “necessary intermediaries between Golbeck and Oracle.” Dkt. 63, at 24–25.
 20 Plaintiffs correctly point out that the mere existence of an intermediary through which a benefit
 21 travels does not doom an unjust enrichment claim under Florida law. Dkt. 67, at 24; *see, e.g.*,
 22 *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1368 (S.D. Fla. 2015). In its
 23 reply papers, Oracle contends there was no direct conferral of a benefit because its third-party
 24 customers merely transmit data to Oracle which Oracle then must process into interest segments
 25 and sell to advertisers. Dkt. 70, at 14.

26 One complication at this stage is that Plaintiffs refer both to the “personal and sensitive
 27 data” Oracle receives, FAC ¶ 251, as well as Oracle’s revenue from selling such data, *id.* ¶ 249, in

explaining how Oracle was unjustly enriched. Oracle, though, does not seem to contest that “data” transferred from one party to another can constitute a benefit.¹³ It comes closest to doing so in its reply papers when it insinuates the benefit must have been revenue earned from data rather than data itself. Dkt. 70, at 14. Even had this issue been squarely addressed by the parties, Florida courts evaluating unjust enrichment claims have found a benefit need not be a clearly defined property interest. *See Cohen v. Kravit Estate Buyers, Inc.*, 843 So.2d 989, 992 (Fla. Dist. Ct. App. 2003) (“No property interest is required.”); *F.H. Paschen, S.N. Nielsen & Assocs. LLC v. B&B Site Dev., Inc.*, 311 So.3d 39, 50 (Fla. Dist. Ct. App. 2021) (asphalt removal and replacement constitutes benefit).

Given that personal data would appear to qualify as a benefit under Florida law, Plaintiffs have a persuasive argument that the presence of intermediaries—here, third-party websites—poses no obstacle to the requirement a benefit be directly conferred. Plaintiffs have averred sufficient facts at this stage that they conferred a direct benefit on Oracle,¹⁴ and, thus, their unjust enrichment claim under Florida law survives.

5. Ninth Cause of Action: Declaratory and Injunctive Relief

Finally, Defendant seeks to dismiss Plaintiffs’ cause of action for declaratory judgment and injunctive relief. This cause of action rises and falls with Plaintiffs’ other claims: if Plaintiffs fail to allege facts sufficient to state a claim under any other cause of action, the claim for declaratory judgment and injunctive relief will be dismissed. Since not all of Plaintiffs’ claims have been dismissed, this cause of action moves forward at this stage.

¹³ At least one court has struggled with what constitutes a “benefit”—where the claimed benefit is not money—in an unjust enrichment claim brought under Florida law in the context of eventually-monetized data. *See Muy v. Int’l Bus. Mach. Corp.*, No. 19-cv-14, 2019 WL 8161745, at *1 (N.D. Fla. July 19, 2019).

¹⁴ It is conceivable further factual development might reveal, for instance, that raw personal data lacks any commercial value before it is “transform[ed].” *See* Dkt. 70, at 14 n.26.

IV. MOTION TO SEAL

Plaintiffs also have a pending administrative motion to seal the OARRRs. *See* Dkt. 75. There is a strong presumption in favor of allowing public access when deciding whether materials should be sealed. *See Apple Inc. v. Psystar Corp.*, 658 F.3d 1150, 1162 (9th Cir. 2011). A request to seal must be narrowly tailored. Civ. L.R. 79-5(c)(3). To overcome the presumption in favor of public access to a judicial record, there generally must be “compelling reasons supported by specific factual findings.” *Kamakana v. City & Cty. of Honolulu*, 447 F.3d 1172, 1178 (9th Cir. 2006) (“The mere fact that the production of records may lead to a litigant's embarrassment, incrimination, or exposure to further litigation will not, without more, compel the court to seal its records.”). Where a litigant presents compelling reasons to seal material, the court must then balance the interests of the public and the party seeking sealing. *Ctr. for Auto Safety v. Chrysler Grp., LLC*, 809 F.3d 1092, 1096–97 (9th Cir. 2016). This balancing test involves such factors as the public’s interest in understanding the functioning of the judicial process and the volume of material sought to be sealed. *See Zakinov v. Ripple Labs, Inc.*, No. 18-cv-6753, 2023 WL 5280193, at *1 (N.D. Cal. Aug. 15, 2023).

Plaintiffs have offered two sets of potential redactions¹⁵ to the OARRRs in response to the direction for more narrowly tailored sealing requests. They argue redactions are necessary to protect Plaintiffs’ privacy because the OARRRs reveal many details about Plaintiffs’ private lives. *See, e.g.*, Dkt. 75, at 5 (listing the types of information the OARRRs reveal). Plaintiffs explain the OARRRs implicate privacy interests in part through the unique “totality of the segments categories attributed” to an individual. *Id.* at 3. In other words, Plaintiffs argue the OARRRs need to be considered both at a micro- (*e.g.*, values for specific categories) and macro-level. Though Defendants did not previously oppose Plaintiffs’ motion to seal, they now argue the information Plaintiffs seek to seal is insufficiently sensitive and that Plaintiffs do not explain how its

¹⁵ Exhibits A and B to the Maher Declaration contain more extensive redactions as compared to Exhibits E and F. Plaintiffs offer the second set of more tailored redactions in case the first set is deemed overly broad. *See* Dkt. 75, at 1.

publication could lead to harm. *See* Dkt. 76, at 2–5. Defendants appear to contest the idea that any of the contested information in the OARRRs is sealable.

On one hand, Plaintiffs’ argument about the privacy interests implicated by the “totality” of attributed segments categories goes too far in that it—if taken to its logical conclusion—would seem to require sealing the OARRRs in their entirety (encompassing terms like “Ad Occurrence”). On the other hand, Plaintiffs’ larger point that the release of a detailed dossier of information about an individual that, by virtue of its comprehensiveness, implicates privacy concerns is compelling. It would be perverse to hold an individual entitled to no protection where a company amalgamates many pieces of information about that individual’s preferences on the grounds that revealing any one preference is no big deal. Plaintiffs clearly have a privacy interest in their “likes, dislikes, interests, and habits over a significant amount of time.” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599 (9th Cir. 2020). Many pieces of information in the OARRRs indicate more than simple likes or dislikes and instead communicate intimate details of Plaintiffs’ daily lives.

For the foregoing reasons, Plaintiffs’ proposed redactions to Exhibits E and F to the Maher Declaration are sufficiently tailored, and Plaintiffs’ motion to seal the OARRRs will be granted to reflect those redactions. Plaintiffs’ privacy interest in the redacted portions of the OARRRs outweighs the public’s interest in fully-disclosed documents in this instance. This is so in part given that the OARRRs, even with redactions, still communicate to the public the types of information that are at issue in this action. Of course, reasonable minds might disagree on distinguishing between which entries in the “Segment Category” column merit sealing and which do not, but Plaintiffs have, at this stage, met their burden to propose a narrowly tailored set of redactions.

V. CONCLUSION

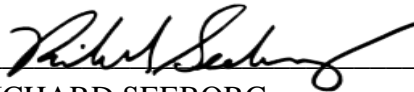
In light of the above, Plaintiffs’ intrusion upon seclusion claim on behalf of the Florida Sub-Class under Florida law is dismissed with leave to amend. To the extent Plaintiffs bring an intrusion upon seclusion claim under California law on behalf of the United States Class, that

1 claim is dismissed without leave to amend. To the extent Plaintiffs bring an unjust enrichment
2 claim under California law on behalf of the United States Class, that claim is dismissed with leave
3 to amend. Additionally, Plaintiffs' ECPA claim is dismissed with leave to amend. Plaintiffs'
4 remaining claims—intrusion upon seclusion under California law on behalf of the California Sub-
5 Class, invasion of privacy, CIPA, FSCA, unjust enrichment, declaratory judgment, and injunctive
6 relief—survive. Plaintiffs are given 20 days to file an amended complaint.

7 Plaintiffs' motion to seal as reflected in the category-by-category redactions in Exhibits E
8 and F to the Maher Declaration is granted. Plaintiffs are ordered to file public versions of both
9 exhibits consistent with this order, no later than October 20, 2023.

10
11 **IT IS SO ORDERED.**

12
13 Dated: October 3, 2023

14 
15 RICHARD SEEBORG
16 Chief United States District Judge
17
18
19
20
21
22
23
24
25
26
27
28